IFW

AF/3621

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Siani Lynne Pearson, et al	)	On Appeal to the Board of Appeals
Patent Application No.: 10/080,479	)	
Filed: 02/22/2002	)	Group Art Unit: 3621
	)	Examiner: Augustin, Evens J
For: "Me thod and Apparatus for Ascertaining The Status of a Data Processing Environment"	)	Date: March 31, 2006

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final Action, dated October 31, 2005, for the above identified patent application. Please deduct the amount of $ 500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief from deposit account no. 08-2025. Appellants submit that this Appeal Brief is being timely filed, since the notice of Appeal was filed on January 30, 2006 and received by the USPTO on February 2, 2006.

04/24/2006 WASFAW1 00000021 082025 10080479
01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC") . HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

Pending Appeal for U.S. S/N 09/979,903 ("Data Integrity Monitoring In trusted Computed Entity") may be related to the present appeal.

Other than that, Appellants submit that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in th e pending appeal.

STATUS OF CLAIMS

Claims 1-24 are currently pending. Claim 11 has been canceled. Claims 1-10 and 12-24 are the subject of this Appeal and are reproduced in the accompanying Claims appendix.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application generally relates to a method of and apparatus for determining the status of a data processing environment (Title, p. 1, lines 6-7 and claims).

This is accomplished by an apparatus for ascertaining the status of a data processing environment, the apparatus comprising at least one trusted computing device (Figs. 1-3, element 2, pages 8-10) which is arranged to challenge other devices (Fig. 2, elements 30, 32, 34, 36, page 9 lines 23-28) within a data processing environment (Figs. 2-3, pages 10-11), to keep a record of the response and to make the record available (Fig. 4, page 11 lines 4-17).

This is also accomplished by a computing device (Fig. 2, element 40, page 9 lines 17-22, page 10 lines 3-14) including a communication device (Fig. 2, element 42, page 9 lines 17-22) and a data processor (Fig. 2, element 44, page 9 lines 17-22), wherein the data processor is arranged to establish communication with a trusted computing device (Fig. 2, element 2, pages 8-10) via the communication device, to receive at least part of the record of responses (Fig. 4, page 11 lines 4-17) and to establish from an internal rules base (Fig. 2, element 46, page 9 lines 20-22) whether the data processing environment is trustworthy enough to enable a class of transaction or task to be carried out in that environment.

A computing device (Fig. 2, element 40, page 9 lines 17-22, page 10 lines 3-14) may also include a communication device (Fig. 2, element 42, page 9 lines 17-22) and a data processor (Fig. 2, element 44, page 9 lines 17-22), wherein the computing device uses the communication device to establish communication with at least one device (Fig. 2, elements 30, 32, 34, 36, page 9 lines 23-28) within a data processing system, and in which the data processor is arranged to identify challenges from at least one trusted computing device (Fig. 2, element 2, pages 8-10), to apply response rules to the challenge and, if a response indicated, to respond to the challenge in accordance with the rules (page 9, lines 17-22).

A method of ascertaining the status of a data processing environment is also provided, comprising the following steps: a trusted computing device (Figs. 1-3, element 2, pages 8-10) challenges other devices (Fig. 2, elements 30, 32, 34, 36, page 9 lines 23-28) within a data processing environment (Figs. 2-3, pages 10-11), keeps a record of responses made to the challenges and makes the record available (Figs. 4-6, pages 11-12).

A method of conducting a transaction in a data processing environment (Figs. 2-3, pages 10-11) comprising a user device (Fig. 3, elements 62, 64, page 10 lines 15-29) and at least a trusted computing device (Fig. 3, element 2, page 10 lines 15-19) each having

respective communication capabilities is further provided, wherein the trusted computing device keeps a record (Figs. 4-6, pages 11-12) of computing devices (Fig. 3, element 60, page 10 lines 15-29) that it has identified within the data processing environment, and whereby the user device establishes communication with the trusted computing device, the trusted computing device sends to the user device at least a portion of the record of computing devices within the data processing environment, and the user device analyses the record to establish what facilitates the user device may access (Figs. 4-6, pages 11-12).

An apparatus for ascertaining the status of a data processing environment is also provided, comprising at least one trusted computing device (Figs. 1-3, element 2, pages 8-10) which is arranged to make periodic challenges (Figs. 5-6, page 12 lines 8-22) to other devices (Fig. 2, elements 30, 32, 34, 36, page 9 lines 23-28) within a data processing environment (Figs. 2-3, pages 10-11), to analyse the responses it receives in order to determine if given devices in the data processing environment are trustworthy, to keep a record of the response and to make the record available to other devices in the data processing environment (Figs. 4-6, pages 11-12).

Further, a method of ascertaining the status of a data processing environment comprises the following steps: a trusted computing device (Figs. 1-3, element 2, pages 8-10) makes multiple challenges to other devices (Fig. 2, elements 30, 32, 34, 36, page 9 lines 23-28) within a data processing environment (Figs. 2-3, pages 10-11), keeps a record of responses made to the challenges, analyses the responses it receives in order to determine if given devices in the data processing environment are trustworthy and makes the record available to other devices in the data processing environment (Figs. 4-6, pages 11-12).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 1-10 and 12-24 are patentable under 35 U.S.C. 102(e) over England, U.S. Patent No. 6,327,652 (hereinafter "England")

ARGUMENT

Issue 1: Whether Claims 1-10 and 12-24 are patentable under 35 U.S.C. 102(e) over England, U.S. Patent No. 6,327,652 (hereinafter "England")

In the final Office Action of October 31, 2005, the Examiner rejects Claims 1-10 and 12-24 under 35 U.S.C. 102(e) as being anticipated by England. Appellants respectfully disagree with the Examiner's rejection for t he following reasons.

Claim 1

A) Claim 1 recites a

"trusted computing devi ce"

while England discloses a server (see box 220 in Figure 2 of England). The Examiner appears to believe that the *"trusted computing device"* of claim 1 is embodied by England's server. See section 4 of the Final Action of October 31, 2005, first bulleted paragraph, where the Examiner makes reference to column 8, line 43 of England.

However, the Examiner has not provided the Appellants with a reasonable basis for the Examiner's belief that England's server 220 is a *"trusted computing device."*

In particular, as noted by Appellants during prosecution of the present application, establishing whether a server is a trusted computing device or not depends on the kind of operation the server intends to perform.

1. The Examiner has tried to expand the basis for the Examiner's reasoning in section 1 of the Final Action of October 31, 2005, where reference has been made to column 8, lines 40-65 of England. According to the Examiner, such passage establishes that the communication process in England uses encryption technology for authentication and therefore makes the client/server communication in England a "trusted" one. In rebuttal, Appellants have the following three observations to offer:

1.1 (use of encryption technology does not mean that a communication is trusted) Column 8, lines 45-47 of England describes Figure 2 of England and states that the arrows between client 200 and server 220 illustrate processes and that many of these processes may incorporate encryption algorithms. However, stating that a process is encrypted does not necessarily mean that the process is "trusted" as the Examiner states. Further, England clearly defines "trusted" as something different from encrypted, i.e. "authenticated as respecting digital rights" (column 8, lines 62-63).

1.2 (Appellants are claiming a *"trusted computing device"*, not a trusted communication) In section 1 of the Final Action of October 31, 2005 the Examiner emphasizes that the client/communication in Figure 2 of England is a trusted one. However, claim 1 recites a *"trusted computing device"*, not a trusted communication. Therefore, the comment of the Examiner does not read on the language of claim 1.

1.3 Appellants also note that the passage of England cited by the Examiner in section 1 of the Final Action of October 31, 2005 includes lines 60-65 of column 8 of England. That passage recites that the "digital rights management operating system (DRMOS) must load and execute only OS components that are authenticated as respecting digital rights ("trusted"), and must allow access to the downloaded content only by similarly trusted applications."

This passage is line with the Appellants' statement that the issue in England is centered on the trustworthiness of the OS component, not on the trustworthiness of the content provided by the server 220. This is made clear, in England, when discussing Figure 2 at columns 9 and 10. Figure 2 shows a server 220 and a client 200. The client 200 comprises a CPU/OS 201 which, in turn, comprises the DRMOS 205. CPU 201 comprises a trusted application 209 (column 9, lines 18-19). Therefore, the trustworthiness at issue in England is that of applications in the CPU/OS 201, such as application 209, and not the trustworthiness of server 220.

2. The Examiner also states that column 15, lines 54-55 of England ("The DRMOS connects on a regular basis to a trusted time server") support the fact that England's server 220 is a trusted one. However, that passage does not refer at all to server 220. To the contrary, it relates to an embodiment where untrustworthy versions have their certificate renewed. See England, column 12, lines 37-52, where use of a "secure time source available on the subscriber computer" (column 12, lines 41-42) is disclosed. Such " secure time source" is clearly not the server 220, as also explained at column 12, lines 43-45: " A monotonic counter in the CPU can serve as this secure time source since it only counts up and cannot be reset "back in time."

B) Claim 1 also recites that

> *"[the] trusted computing device is arranged . . . to keep a record of the response."*

In the Action of April 21, 2005, the Examiner appears to identify this feature in two different places of England, both of which, however, do not correspond to the recited feature.

Firstly, the Examiner asserts that a log or historical status of the user devices is also being kept in England (see column 13, lines 54-59 of England). Although the statement is correct as such, the Examiner fails to mention that the record is kept in the CPU 201 of the client 200 and not in the server 220. In other words, even assuming, *arguendo*, that the Examiner is right in stating that a server is a trusted computing device, England' s server does not keep a record of the response as recited in claim 1.

Second, the Examiner also states that England's server 220 stores (or keeps record) of an "acce ss predicate" which the server makes available with the content 221 sent to the client 200, thus implying that England anticipates the feature *"[th e] trusted computing device is arranged . . . to keep a record of the response and to make the record available"* of claim 1. However, this is not what happens in England.

An "acce ss predicate" as defined in England is not a record of the response stored in the server. Looking at Figures 10 and 11 (and the corresponding portion of the specification, column 19, line 6 through column 20, line 13) of England, it is apparent that the access predicate is a list of conditions to which the client must satisfy in order to obtain the content. For example, is the client within a specified trust level field?

(elements 1001-1003) Has the client derivation rights or rights to allow the content to be sent to other clients? (Figure 11). Therefore, such list of conditions is not a *"record of the response."*

C) Regretfully, in the Final Action of October 31, 2005, the Examiner offers no comment at all in response to Appellants' arguments as to feature B) of claim 1. Therefore, in doing so, the Examiner has not complied with 37 CFR 1.104(c)(2), which states as follows:

> "In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes invention other than that claimed by Applicant, the particular part relied on must be **designated as nearly as practicable**. The pertinence, if not apparent, must be clearly explained and each rejected claim specified" (emphasis added)

Appellants submit that the Examiner has failed to "designate as nearly as practicable" the particular part of England relied upon in making the assertion that England discloses *"[the] trusted computing device is arranged . . . to keep a record of the response."*

Hence, Claim 1 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claims 2, 3, 5-10

Appellants submit that Claims 2, 3, and 5-10, at least based on their dependency on Claim 1, are patentable over England.

Claim 4

1) Appellants submit that Claim 4, at least based on its dependency on Claim 1, is

patentable over England.

2) Appellants also submit that England does not disclose, suggest or teach at least the following features recited by Claim 4 of the present application:

> *"the at least one trusted computing device is arranged to listen to communications within the data processing environment so as to identify the presence of new devices"* (emphasis added).

In the Actions of April 21, 2005 and October 31, 2005 the Examiner states that column 9, lines 48-51 of England discloses a response message transmitted to the server, that includes the identity of user devices. However, transmission of the identity 206 of CPU 201 (see Figure 2 of England) just allows the server 220 to understand that the message is coming from CPU 201, not *"to identify the presence of new dev ices"* as claimed.

Hence, Claim 4 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claim 12

Appellants submit that England does not disclose, suggest or teach, *inter alia*, the following feature recited by Claim 12 of the present application:

> *"wherein the data processor is arranged to establish communication with a trusted computing device"* (emphasis added)

Appellants make reference to the arguments presented with reference to claim 1 as to the presence of the *"trusted computing devi ce"* feature.

Hence, Claim 12 is patentable over England and the Examiner's rejection should be

reversed on appeal.

Claim 13

Appellants submit that England does not disclose, suggest or teach, *inter alia*, the following feature recited by Claim 13 of the present application:

> *"in which the data processor is arranged to identify challenges from at least one trusted computing device"* (emphasis added)

Appellants make reference to the arguments presented with reference to claim 1 as to the presence of the *"trusted computing devi ce"* feature.

Hence, Claim 13 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claim 14

1) Appellants submit that claim 14, at least based on its dependency on claim 13, is patentable over England.

2) Appellants also submit that England does not disclose, suggest or teach, *inter alia*, the following features recited by Claim 14 of the present application:

"the computing device is arranged to search for a generation identifier within the challenge, to apply response rules to the generation identifier to see if the challenge is still valid, and if it is not to disregard the challenge" (emphasis added).

In the Actions of April 21, 2005 and October 31, 2005 the Examiner makes reference to sections of England where the CPU 209 of Figure 2 is provided with a monotonic counter as a secure time source (see column 12, lines 43-52, column 15, lines 50-60 and column 19, lines 45-49 of England). Those passages have nothing to do with challenges between a computing device and a trusted computing device. To the contrary, they deal with the way a certificate of a component is renewed.

Hence, Claim 14 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claim 15

1) Appellants submit that claim 15, at least based on its dependency on claim 14, is patentable over England.

2) Appellants also submit that England does not disclose, suggest or teach, *inter alia*, the following features recited by Claim 15 of the present application:

"the computing device retransmits the challenge with a modified generation identifier if the challenge is valid" (emphasis added)

As already explained with reference to claim 14, the Examiner makes reference to sections of England where the CPU 209 of Figure 2 is provided with a monotonic counter as a secure time source (see column 12, lines 43-52, column 15, lines 50-60 and column 19, lines 45-49 of England). Those passages have nothing to do with challenges between a computing device and a trusted computing device. To the contrary, they deal with the way a certificate of a component is renewed.

Hence, Claim 15 is patentable over England and the Examiner's rejection should be

reversed on appeal.

Claim 16

A) Claim 16 recites a

> *"trusted computing devi ce".*

Appellants make reference to the arguments presented with reference to claim 1 as to the presence of the *"trusted computing devi ce"* feature.

B) Claim 16 further recites that

> the *"trusted computing device . . . keeps a record of responses made to the challenges"* (emphasis added)

Appellants make reference to the arguments presented with reference to claim 1 as to the presence of the *"record of responses"* feature.

Hence, Claim 16 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claims 17, 18

Appellants submit that Claims 17 and 18, at least based on their dependency on Claim 16, are patentable over England.

Claim 19

1) Appellants submit that Claim 19, at least based on its dependency on Claim 16, is patentable over England.

2) Appellants also submit that England does not disclose, suggest or teach at least the following features recited by Claim 19 of the present application:

> *"the at least one trusted computing device listens to communications within the data processing environment so as to identify the presence of new devices"* (emphasis added).

Appellants make reference to the arguments presented with reference to claim 4.

Hence, Claim 19 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claim 20

1) Appellants submit that claim 20, at least based on its dependency on claim 16, is patentable over England.

2) Appellants also submit that England does not disclose, suggest or teach, *inter alia,* the following features recited by Claim 20 of the present application:

"such that any device receiving the challenge can examine the generation identifier in order to establish whether the challenge is directly received from the trusted computing device or whether it has been retransmitted." (emphasis added).

In the Actions of April 21, 2005 and October 31, 2005, the Examiner mentions the passages at column 19, lines 15-39 and column 10, lines 14-17. However, none of those

passages disclose a discrimination between challenges directly received from the trusted computing device or retransmitted.

Hence, Claim 20 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claim 21

A) Claim 21 recites a

"trusted computing devi ce"

Appellants make reference to the arguments presented with reference to claim 1 as to the presence of such feature.

B) Claim 21 further recites that

> *"the trusted computing device keeps a record of computing devices that it has identified within the data processing environment"*

Appellants make reference to the arguments presented with reference to claim 1 as to the presence of such feature. In particular, in the passage at column 13, lines 54-59 of England cited by the Examiner, a boot log is maintained in the DRMOS of the client 200, and not in the server 220. Further, an access predicate (as disclosed in England) is not "a record of computing devices." Reference is made again to the arguments presented with reference to claim 1.

Hence, Claim 21 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claim 22

1) Appellants submit that Claim 22, at least based on its dependency on Claim 21, is patentable over England.

2) Appellants also submit that England does not disclose, suggest or teach at least the following features recited by Claim 22 of the present application:

> *"the user device further analyses the record in accordance with a se t of security rules to determine what level of trust can be placed on the integrity of the data processing environment."*

Claim 22 puts the emphasis on the way the user device analyses the level of trust of the data processing environment. The Examiner makes reference to column 9, lines 52-55 and column 10, lines 14-17 of England. However, column 10, lines 14-17 discloses interactions between the server 220 and the client 200 in England, not the level of trust that the user device can place on the integrity of the data processing environment. Further, column 9, lines 52-55 talks about " common protocols" as the Examiner also points out. How can the generic wording "common protocols" be an anticipation of *"security rules to determine what level of trust can be placed on the integrity of the data processing environmen"* ? Such feature is clearly not disclosed in England.

Hence, Claim 22 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claim 23

A) Claim 23 recites a

"trusted computing devi ce"

B) Claim 23 further recites that

> the *"trusted computing device . . . is arranged . . . to keep a record of the response and to make the record available to other devices in the data processing environment."*

In both cases A) and B), Appellants make reference to the arguments presented with reference to claim 1 as to presence of the above recited features.

Hence, claim 23 is patentable over England and the Examiner's rejection should be reversed on appeal.

Claim 24

Claim 24 recites

> *"a trusted computing device" that "keeps a record of responses made to . . . challenges, analyses the responses it receives in order to determine if given devices in the data processing environment are trustworthy and makes the record available to other devices in the data processing environment."*

Appellants make reference to the arguments presented with reference to claim 1 as to presence of the above recited features.

Hence, Claim 24 is patentable over England and the Examiner's rejection should be reversed on appeal.

* * *

Conclusion

For the extensive reasons advanced above, Appellants respectfully contend that each claim is patentable. Therefore, reversal of all rejections and objections is courteously solicited.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

March 31, 2006
(Date of Transmission)

Shannon Tinsley
(Name of Person Transmitting)

Shinsley
(Signature)

3/31/06
(Date)

Respectfully submitted,

Alessandro Steinfl
Attorney for the Applicant
Reg. No. 56,448
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile

Encls.:
- Appendices A, B and C
- Postcard

1. (original) An apparatus for ascertaining the status of a data processing environment, comprising at least one trusted computing device which is arranged to challenge other devices within a data processing environment, to keep a record of the response and to make the record available.

2. (original) An apparatus as claimed in claim 1, in which the trusted computing device is arranged to make periodic challenges to the other devices in order to maintain the accuracy of the record.

3. (original) An apparatus as claimed in claim 1, in which the record indicates the historical status of the data processing environment.

4. (original) An apparatus as claimed in claim 1, in which the at least one trusted computing device is arranged to listen to communications within the data processing environment so as to identify the presence of new devices.

5. (original) An apparatus as claimed in claim 1, in which the record includes data identifying the type of devices in the data processing environment.

6. (original) An apparatus as claimed in claim 1, in which the trusted computing device is arranged to analyse the responses it receives in order to determine if a given device in the data processing environment is trustworthy.

7. (original) An apparatus as claimed in claim 6, in which the record indicates whether a device has been judged as trustworthy by the trusted computing device.

8. (original) An apparatus as claimed in claim 1, in which the at least one trusted computing device acts as a gateway to the data processing environment.

9. (original) An apparatus as claimed in claim 1, in which the at least one trusted computing device is a server.

10. (original) An apparatus as claimed in claim 1 in which the at least one trusted computing device transmits a challenge which includes a generation identifier which enables devices receiving the challenge to identify whether the challenge is valid.

11. (canceled)

12. (original) A computing device including a communication device and a data processor, wherein the data processor is arranged to establish communication with a trusted computing device via the communication device, to receive at least part of the record of responses and to establish from an internal rules base whether the data processing environment is trustworthy enough to enable a class of transaction or task to be carried out in that environment.

13. (original) A computing device including a communication device and a data processor, wherein the computing device uses the communication device to establish communication with at least one device within a data processing system, and in which the data processor is arranged to identify challenges from at least one trusted computing device, to apply response rules to the challenge and, if a response indicated, to respond to the challenge in accordance with the rules.

14. (original) A computing device as claimed in claim 13, in which the computing device is arranged to search for a generation identifier within the challenge, to apply response

rules to the generation identifier to see if the challenge is still valid, and if it is not to disregard the challenge.

15. (original) A computing device as claimed in claim 14, in which the computing device retransmits the challenge with a modified generation identifier if the challenge is valid.

16. (original) A method of ascertaining the status of a data processing environment, comprising the following steps: a trusted computing device challenges other devices within a data processing environment, keeps a record of responses made to the challenges and makes the record available.

17. (original) A method as claimed in claim 16, in which the trusted computing continues to challenge the devices in the data processing environment so as to maintain an evolving record of the status of the data processing environment.

18. (original) A method as claimed in claim 16, in which the record includes a historical status of the data processing environment.

19. (original) A method as claimed in claim 16, in which the at least one trusted computing device listens to communications within the data processing environment so as to identify the presence of new devices.

20. (original) A method as claimed in claim 16, in which the challenge generated by the trusted device includes a generation identifier such that any device receiving the challenge can examine the generation identifier in order to establish whether the challenge is directly received from the trusted computing device or whether it has been retransmitted.

21. (original) A method of conducting a transaction in a data processing environment comprising a user device and at least a trusted computing device each having respective communication capabilities wherein the trusted computing device keeps a record of computing devices that it has identified within the data processing environment, and whereby the user device establishes communication with the trusted computing device, the trusted computing device sends to the user device at least a portion of the record of computing devices within the data processing environment, and the user device analyses the record to establish what facilitates the user device may access.

22. (original) A method of conducting a transaction as claimed in claim 21, wherein the user device further analyses the record in accordance with a set of security rules to determine what level of trust can be placed on the integrity of the data processing environment.

23. (original) An apparatus for ascertaining the status of a data processing environment, comprising at least one trusted computing device which is arranged to make periodic challenges to other devices within a data processing environment, to analyse the responses it receives in order to determine if given devices in the data processing environment are trustworthy, to keep a record of the response and to make the record available to other devices in the data processing environment.

24. (original) A method of ascertaining the status of a data processing environment, comprising the following steps: a trusted computing device makes multiple challenges to other devices within a data processing environment, keeps a record of responses made to the challenges, analyses the responses it receives in order to determine if given

devices in the data processing environment are trustworthy and makes the record available to other devices in the data processing environment.

*****

There is no evidence submitted with the present Brief on Appeal.

No copies of decisions rendered in related proceedings are being submitted.